Privacy Act Newsletter

1 Oct 2014   **Volume 1, Issue 2**

Did You Know?

- E-mails containing FOUO/PII must be signed and encrypted

- DSET was first introduced to the Air Force in 2009

- DSET not only scans composed messages but attachments as well

- There is an Air Force Blocked Attachment List

- DSET will ultimately be able to scan for a variety of PII

Digital Signature Enforcement Tool (DSET)

Digital Signature Enforcement Tool, also known as DSET, is an e-mail tool being revamped in order to reduce breaches of personally identifiable information (PII) Air Force wide. Initially, DSET was used to palliate risk from e-mail scams and phishing attacks. It was first introduced by the Air Force Life Cycle Management Center and was a feature in Microsoft Office in 2009.

Currently, DSET reminds Air Force users to double check e-mails for PII and For Official Use Only (FOUO) information. This tool scans and detects hyperlinks and attachments in e-mails that might possibly contain sensitive information and notifies the user before the e-mail is sent. The purpose of DSET is to provide an extra layer of protection when messages are sent with PII and FOUO information. With this Microsoft add-on, users are more aware of protecting PII via e-mail.

DSET is equipped with many features to aid with the reduction of PII breaches. In Outlook, two icons are provided in the message toolbar that are labeled "Contains FOUO" and "Contains PII." These icons are located next to the "Sign" and "Encrypt" icons. If the user doesn't initiate the proper steps to digitally sign and encrypt the message containing FOUO or PII, a window will pop-up prompting the user to do so. DSET will scan e-mails for number combinations that may possibly be Social Security Numbers (SSN) and the user can confirm whether or not it contains PII. The purpose of this tool is not only to protect PII, but to also make Air Force users more aware. Air Force users should be more involved in the course of action being taken in order to prevent PII breaches. The user should be checking their e-mails frequently to make sure they are not improperly releasing PII. Alonzo Pugh, cyber business system analyst for the 24th AF, states, "When users release PII that is not protected, that puts information at risk for being intercepted by adversaries. These adversaries can then use that information to target users to gain access to the network." It is the job of all Air Force users to protect PII.

Will DSET Work On Organizational Accounts?

Organizational accounts that have been validated by their units are currently able to encrypt e-mails containing FOUO and PII. DSET will be applicable to organizational e-mail accounts meaning that messages sent with PII or FOUO information need to be signed and encrypted, a feature that was not previously used in Microsoft Office. Many of these accounts are used for Decoration Packages and Evaluation Reports which are considered FOUO and include PII so senders must be sure to properly protect this information. Sponsors for organizational e-mail accounts must ensure that their accounts have up-to-date e-mail encryption certificates. For more in-depth information on this subject, please contact the 4 CS Communications Focal Point at DSN 722-2666.

Knowledge Management Center

4 CS/SCXK
1290 Jabara Ave
Seymour Johnson AFB, NC 27531

Contact Us:
DSN: 722-8484
4cs.scxk.knowledgemanagementcenter@us.af.mil

DSET Features

One additional DSET feature has the ability to scan attachment file types in e-mails and block possible at-risk attachments. If any of the e-mail's attachments are on the Air Force block list, there will be a pop-up providing two options. The first option will say "Continue Anyway" which allows you to send the at-risk attachment. Although you continued to send the e-mail, the receiver may not be able to view the attachment. The second option will say "Cancel," and it will bring the composer back to the draft e-mail to either discard the attachments or change the file format. By not being able to send attachments that are listed on the Air Force Blocked Attachment list allows users to eliminate the risk of breaches through Air Force networks.

Another DSET feature will alert the sender if the recipient is on a domain that isn't approved to receive PII or FOUO information. The sender is presented with an alert (image to the left) to either remove or keep the recipient. If the sender chooses to keep the recipient, the e-mail will be sent but the PII or FOUO information will not be included in the message. The recipient also may not receive the message altogether.

There are a plethora of features associated with the DSET tool to ensure that PII is being protected when sending out e-mail messages. Below are more additional features within DSET.

Additional Features
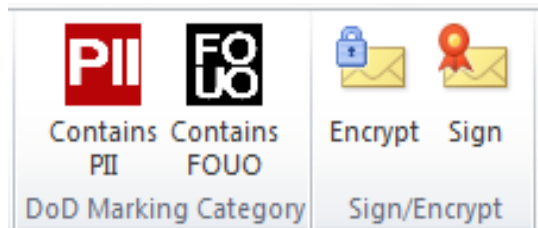
The image at the top left is an example of the icons that are in the message toolbar. If users aren't proactive about identifying PII or FOUO in their message, DSET will prompt the user to confirm if there is PII or FOUO information in the message. If the user is proactive and identifies that the message contains PII and/or FOUO, there will be no pop-up window. Although the user identifies PII and FOUO, the user still must sign and encrypt the email to protect the information. Before the message is sent out, the DSET plug-in will scan the message, along with any attachments and hyperlinks and prompt pop-up windows to warn the user of potential PII. The pop-up window gives the user the option to "View Potential PII" to see what DSET has detected as potential PII. It will show any potential PII that may be in the attachment or the body of the e-mail message. When this window pops up, the user can "redact" any PII or simply delete the attachment containing the potential PII data. If the user chooses the option to "Redact in Subject Line and Message Body," the identified information becomes blacked out (see image to the bottom left).
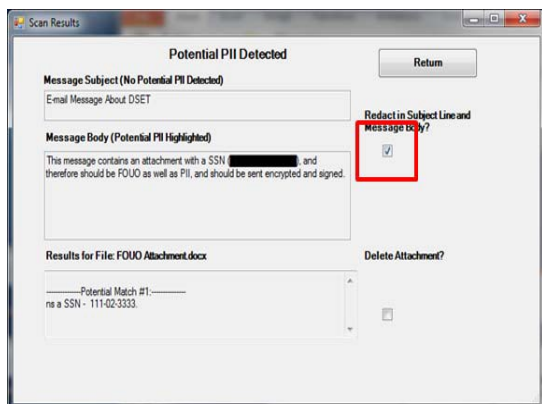
These are just a few of the many features of the DSET program. These features are all used in conjunction to better help Air Force users better safeguard PII.